A Microgrid Testbed for Interdisciplinary Research on Cyber-Secure Industrial Control in Power Systems

A Microgrid Testbed for Interdisciplinary Research on Cyber-Secure Industrial Control in Power Systems

David M Laverty, Mats-Robin Jacobsen, Xiaodong Zhao
Queen's University Belfast
School of EEECS, Ashby Building
125 Stranmillis Road, Belfast, UK
+44 (0) 28 9097 4651
david.laverty@qub.ac.uk
mjacobsen02@qub.ac.uk
xzhao06@qub.ac.uk

Kieran McLaughlin, Ivo Friedberg, Rafiullah Khan, Sakir Sezer
Centre for Secure Information Technologies (CSIT)
Queen's University Belfast
+44 (0) 28 9097 1890
kieran.mclaughlin@qub.ac.uk
ifriedberg01@qub.ac.uk
rafiullah.khan@qub.ac.uk
s.sezer@ecit.qub.ac.uk

ABSTRACT
This paper describes a smart grid test bed comprising embedded generation, phasor measurement units (PMUs), and supporting ICT components and infrastructure. The test bed enables the development of a use case focused on a synchronous islanding scenario, where the embedded generation becomes islanded from the mains supply. Due to the provisioned control components, control strategy, and best-practice ICT support infrastructure, the islanded portion of the grid is able to continue to operate in a secure and dependable manner.

CCS Concepts
• Computer systems organization → Embedded and cyber-physical systems → Sensors and actuators • Security and privacy → Systems security • Hardware → Power and energy.

Keywords
Testbed; Smart Grid; secure control; microgrid; synchronous-islanding

1. INTRODUCTION
'Smart Grid' is a wide encompassing term, but applications falling into this category generally refer to the application of modern Information Communication Technology (ICT) to solve challenges and constraints in the operation of traditional electrical energy infrastructure. Whilst there are many decades of experience of the application of ICT at transmission system voltages, where there was a clear business case for dedicated utility own communications, there is now momentum behind the application of such applications at lower distribution level voltages. At these voltage levels, the business case for dedicated communications is not clear, and it is generally necessary to make use of public telecoms infrastructure. While these novel methodologies are needed to allow existing infrastructure to fulfill a changing role, the operation of critical control algorithms on ICT infrastructure, and in particular public ICT infrastructure, introduces the risk of cyber-attacks that can cause physical damage.

The relationship between the traditional safety domain and the cyber security domain is a major challenge for the acceptance of 'smart grid' solutions. It is a challenge that cannot be sufficiently addressed by the necessary application of existing solutions from either domain [13]. In the CAPRICA project the authors investigate how control algorithms can be designed to be resilient in the face of cyber-attacks. Further, the authors develop ICT solutions that make use of the best practice in the traditional ICT domain.

Of particular interest to electrical energy networks at present, notably across Europe and in particular the authors' home network on the island of Ireland, is the issue of the integration of renewable electricity generation. At the time of writing, the all-Ireland power system frequently meets demand with as much as 50% of supply coming from non-synchronous machine generators, predominately made up of wind generation [1]. The issues that arise, including reduction in system inertia and changing fault levels, was not foreseen when the architecture of the electrical infrastructure was designed in the 1950s/60s/70s when centralize bulk generators supplied by fossil fuels was the norm. Hence, there is a requirement for novel methods of power system operation to enable the system to function with this and higher levels of system non-synchronous penetration (SNSP).

The authors' have an interested in a state of power system operation known as 'synchronous islanding' [2]. Conventionally, power system islanding is a mode of operation to be avoided, as is the case in the authors' complimentary research work in islanding protection [3]. However when an island is appropriately controlled, the dangers of uncontrolled islanding are avoided and there is a benefit to the utility in terms of reduction in customer minutes lost, and generation is kept online avoiding the need for it to be disconnected, shut down, and restarted.

In this paper the authors present a physical electrical system testbed, representing a microgrid containing embedded generation, that has been built at Queen's University Belfast (QUB). The testbed was originally constructed to demonstrate the feasibility of synchronous islanding of a single machine, then adapted for multi-machine islanding, and then again to create a testbed on which to investigate the interdisciplinary domain of cyber-secure industrial control systems (see Section 2). The authors will describe the detailed testbed setup in Section 3 together with possible cooperation opportunities. Section 4 will highlight the authors' current research that is performed on the testbed before concluding the paper in Section 5.

2. THE USE CASE
Due to the geographical location of the resource, large scale renewable electricity sources are predominantly located in isolated areas. This presents a challenge to the successful integration of renewable electricity generators, since such remote areas tend to be weakly electrically connected. That is there is no access to the bulk transmission grid, rather power must be transferred at lower voltages across the distribution network. Issues arise including that of voltage rise, power quality and flicker, and constraints and

bottlenecks caused by the capacity of the infrastructure to accommodate reverse power flows. Amongst these challenges is the issue of islanding.

Islanding is the scenario in which an embedded generator (that is, a small generator connected to the distribution network) finds itself operating without connection to bulk utility dispatched generation. This is often caused be a fault upstream of the generator being cleared (disconnected) by the correct operation of protection systems (circuit breakers open). See Figure 1. When a generator operates in an island, there is the possibility for it to supply utility customers outside of the generator owner's premises. This presents a risk to the other customers due to lack of regulation of voltage and frequency, a risk to utility personnel restoring the fault (who would assume the downstream side to be de-energized) and risks the destruction of the embedded generator is reconnection is made out of synchronism with the mains supply.

A generator must be connected to the mains under a process called 'synchronization', during which the voltage of the generator is matched to that of the mains, the frequency is matched to that of the mains, and the phase angle of the voltage is matched to that of the mains. Should any of these properties be incorrect, the generator cannot synchronize due to risks of severe damage to the equipment and personnel safety. For these reasons, islanding is forbidden on most systems.

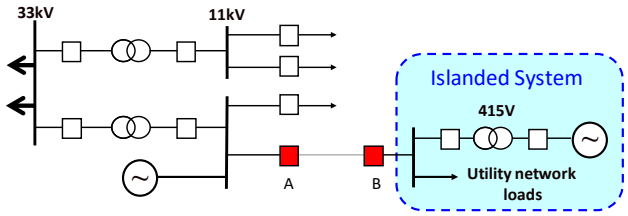

Figure 1: Example Islanding Scenario

The incumbent forms of islanding detection in use today are Rate-of-Change-of-Frequency (ROCOF) and Vector Shift. A thorough technical description of these technologies is outside the scope of this paper, but in summary these technologies are no longer fit to serve on modern grids. Both technologies were designed for use on grids with low penetrations of embedded generation, and known deficiencies that could lead to nuisance tripping (that is, disconnecting a generator when there was no need to) had virtually no impact on the wider system. In the present day, the widespread use of embedded generation means that these technologies must be desensitized otherwise nuisance tripping would be frequent, and the potential for one nuisance trip to cause further 'cascade tripping' and loss of system supply is now of concern. Consequently, novel methods of determining when a generator has become disconnect from the mains (known as 'loss-of-mains' or islanding) is an active research domain [3].

A contrary viewpoint to disconnecting a generator once islanding has been identified is that if one were to control the generator so that it was held artificially in synchronism with the utility grid, then the risks of out-of-synchronism reconnection of the generator are mitigated. Issues of power quality are intrinsically addressed, and those of personnel safety would be resolved through staff training.

Synchronous islanding is made possible by the application of time synchronized phasor measurements, known as synchrophasors. A phasor represents the amplitude, frequency and phase angle of a voltage or current on a power system. Synchrophasors are phasors acquired by a device disciplined to the UTC timebase (typically using a GPS receiver), such that measurements can be taken over a wide geographical area and then usefully compared.

In a synchronous island, the embedded generator operates a control loop to match the properties of a phasor acquired at the generator terminals to a phasor representing a reference location. A suitable reference location would be a highly interconnect substation.

Prior work has considered the physical aspects of the synchronous islanding problem, and identified useful technical design parameters. For example, the system shall fail if the phase angle diverges beyond ±60° [4], or if the telecoms delay becomes longer than 300ms [2].

A current parallel activity is investigating a physical demonstration of multi-generator synchronous islanding, which necessitates a further supervisory control loop with telecommunication between generators. This was previous presented as a simulation exercise [5], where the ICT was considered ideal to allow emphasis on the physical challenge. The physical demonstrator must address the role of ICT.

The quality of the phasor measurements themselves are important which has prompted the authors to develop their own phasor measurement unit. The original version of this work has been open sourced with further details in [7]. A new version, which has been constructed in a modular manner specifically to enable interdisciplinary collaboration, is in the final stages of development. This new version the OpenPMU is split into three modules; data acquisition, signal processing, and telecommunications. This allows subject experts to contribute to their module, with a simple API between each module. This yields a technology platform that is highly suitable to develop further 'smart grid' applications in addition to the PMU function.

In this work, it is important to consider that the present standard governing PMU telecommunications, IEEE Std. C37.118.2 [6] provides no intrinsic security mechanisms, instead passing responsibility for security to the network. The modular design of the PMU used in this work allows state-of-the-art security mechanisms to be designed intrinsically into the measurement technology.

This work investigates the link between the cyber domain and the physical domain. High quality measurement technology allows measurement error to be discounted so that small signal analysis of control loop response can yield information as to the state-of-health of the telecoms network, potentially providing a mechanism to identify unauthorized intrusion or manipulation of the sensor data.

To investigate these challenges, the authors have implemented a testbed that allows for the evaluation of novel control algorithms for various Smart Grid use cases from a control and an ICT perspective. Currently the authors are focusing on the synchronous islanding problem but the capabilities of the testbed are not limited to this use case.

3. TESTBED DESCRIPTION

The laboratory setup consists of one load bank, two generator sets, a transmission line model, two synchrophasor measurement units (which can be standard commercial equipment or they could be OpenPMUs described in [6]) and a tie to the main utility grid. A simplified schematic is shown in Figure 2. One of the synchrophasor measurement units is connected to the islanded area, and the other to the main utility grid providing a reference angle for the controller of the islanded area to steer the islanded area towards. Alternatively one could skip the main utility grid synchrophasor unit and provide a stream of historical synchrophasor

measurements that would act as the reference for the setup. Figure 3 shows an overview of the laboratory setup.

The laboratory test setup contains two generator sets which will be used to mimic the behaviour of hydro-electric generation. These generator sets are built by Scott & CO. A 7.5 bhp 1500 RPM DC machine acts as the turbine providing mechanical torque, coupled to a 3 phase 5 kVA 2 pole pair synchronous machine acting as the generator.

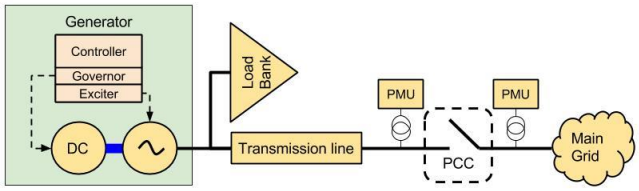

Figure 2: Schematic of laboratory setup of single machine synchronous island

The generator sets have two main ways of providing controllability to the laboratory setup; adjusting the torque provided by the DC machine effectively changing the active power output of the generator and controlling the excitation current in the synchronous machine which will lead a change of reactive power produced or drawn by the generator.

In order to control the generator sets in the laboratory environment a mini-computer, a Raspberry Pi [9], is provisioned to act as a controller for each set (Fig. 4). The Raspberry Pi functions as the turbine governor and the automatic voltage regulator, controlling the torque of the generator set. It controls the generator set in such a way that the response mimics the response of the power plant it represents, in this case a hydro power plant.

The authors have chosen to add a Pulse Width Modulation (PWM) add-on card to the Raspberry Pi to allow the control of both the 'Eurotherm DC machine controller' and the excitation current for the synchronous machine. The 'Eurotherm DC machine controller' requires a smooth voltage input from 0-10 V in order to function correctly so a simple operation amplifier low pass filer circuit was required to smoothen out the PWM signal generated by the Raspberry Pi add-on card. The operation amplifier also amplifies the voltage by two effectively increasing the output voltage from 0-5 V to 0-10 V.

In order to control the generator shown in Figure 3 a hardware controller was built. The hardware controller utilizes a 'Raspberry Pi 2' as the main computation unit and a micro controller, the Teensy 3.2 [8], as an input/output device that allows the Raspberry Pi to send set-point adjustments to the generator and receive feedback required by the automatic voltage regulator. The Raspberry Pi runs a Python code that controls the generator set such that the generator set mimics the operation of a hydro-electric generator set. This is implemented using time constants to the control input providing the generator set with longer response time.

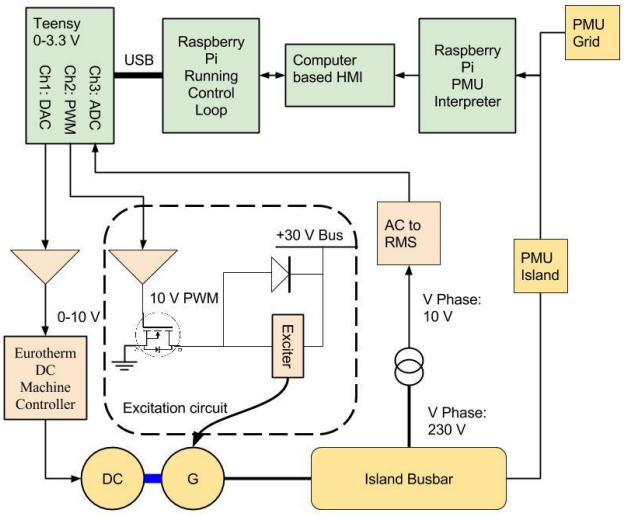

Figure 3: Overview of controller implementation

4. A MODULARIZED PMU

It has been found that present commercially available PMU equipment has unsatisfactory performance. The development of novel real-time control in this work is reliant on the quality of the sensing and feedback apparatus. It was identified early in the work that it would be necessary for the authors to build upon their existing work on the 'OpenPMU' and produce a high quality instrument. The authors' have modularized the functions of the OpenPMU into three major distinct functions. These are data acquisition, signal processing, and data representation (telecommunications), as depicted in Figure 4.

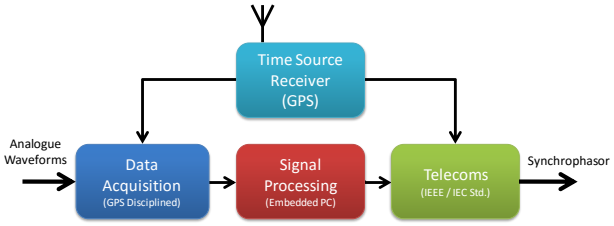

Figure 4: The major components of the OpenPMU system

By modularizing the functions of a PMU, this allows subject experts to focus their efforts on the area of PMU technology to which they can best contribute. The data acquisition stage requires a subject expert in ADC devices, hard-real-time programming environments and time transfer. The signal processing stage is essentially a mathematical problem that can be offloaded to a powerful CPU; subject experts in phase estimation algorithms can apply their expertise here. The telecoms component requires a subject expert in network communications, historians/databases and security.

The interface between each module is achieved using XML datagrams, transmitted by UDP. When two functions appear on the same machine, the operating system's local loopback address is used. All data is presented with human readable tags, and in ASCII format. This is bandwidth inefficient, but allows for extensive interoperability and reduces the learning curve for new contributors. Bandwidth efficient can be improved by adopting JSON in favor of XML. An example of a datagram containing raw waveform sample data is presented in Figure 5. The waveform was

acquired at 12.8 kHz, 16-bits, then formatted into Base64. This section shows 10 ms worth of sample data.

```
<?xml version="1.0" encoding="UTF-8"?>
<OpenPMU>
    <Format>Samples</Format>
    <Date>2015-06-30</Date>
    <Time>10:18:07.460</Time>
    <Frame>23</Frame>
    <Fs>12800</Fs>
    <n>256</n>
    <bits>16</bits>
    <Channels>3</Channels>
    <Channel_0>
        <Name>Belfast_Va</Name>
        <Type>V</Type>
        <Phase>a</Phase>
        <Range>275</Range>
        <Samples>
        VWxJVG5CaVYyeHpXVmhKWjFwWE5XcGlNbEp3WW0xaloyTXlUbT
        lhVnpGc1kzbENNR0ZIUmpCS1IxWjFXVEk1YTFwVFFtbGhWelZv
        WTI1cloxcEhSakJaVTBKcFpWTkNNR050Vm1oa1IyeDFXbmxDY0
        dSRFFuVmtWekZzWTIxc2FsbFhlSE5sVTBKb11tMVJaMlJJU21o
        aWJrNXpXVmhTY0dKdFkyZGhXRkZuWVZjMU1HSjVRbWhKUjBwb1
        l6S1ZaMDVxVVdkamJWWjNZMjFXZWxwWE4=</Samples>
    </Channel_0>
</OpenPMU>
```

Figure 5: Example XML Datagram

This modular platform has potential as a Smart Grid development platform beyond PMU devices, with applications in Smart Metering, Demand Side Management and Power Quality in development.

4.1 Secure Communication Framework

To ensure secure and reliable communication, the developed communication framework is based on IEC 61850-90-5 [10]. The protocol stack for IEC 61850-90-5 standard is depicted in Figure 6 that highlights it evolution from substation automation standard i.e., IEC 61850. The synchrophasor measurements are transmitted using Sampled Values (SV). SV is a stream based messaging protocol designed for high speed sharing of information across the system for time-critical applications.

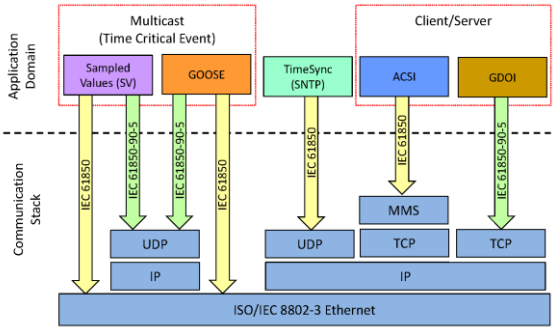

Figure 6: Protocol stack of IEC 61850-90-5

The SV messages are protected by a security mechanism known as Group Domain of Interpretation (GDOI) [11]. GDOI provides enhanced security and protection against man-in-the-middle, connection hijacking, replay, reflection and denial-of-service attacks. It is a group key management protocol that relies on ISAKMP for secure authentication of communicating peers over an insecure wide-area network. The key establishment mechanism of our communication framework is based on Diffie Hellman exchange which is one of the most successful protocol for public key cryptography [12]. The GDOI mechanism assigns Security Association (SA) to communicating peers based on information stream, destination Ethernet or IP address and content/service type. Further, each SA has a certain validity and is refreshed periodically to achieve best possible protection against cryptanalysis. IEC 61850-90-5 along with the distinguishing features of GDOI makes it the well suited communication framework for protecting the critical infrastructure involved in the synchrophasor applications.

4.2 Increased Accuracy of Phasor Measurement Units for Grid Control

As a core part of the phasor measurement units, the data acquisition block in Figure 4 is specially designed to utilize the widely available GPS signal. As illustrated in Figure 7, it consists of four components: a BeagleBone black development board as the main processing unit, a GPS receiver providing the required time information and synchronization, a phase locked loop (PLL) tracked on the UTC time and producing the data sampling clock, and finally an analogue to digital converter digitalizing the input phasors.

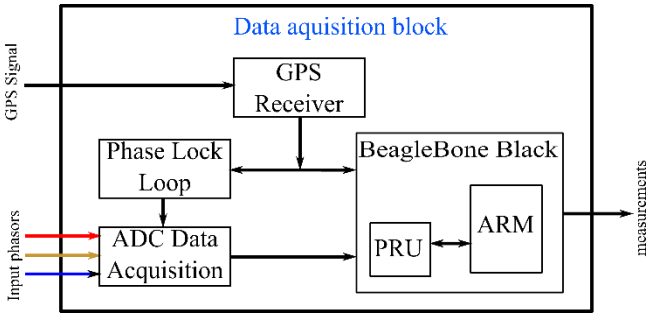

Figure 7: Data acquisition block structure

The GPS receiver provides a pulse signal every second, which can be used to synchronize the start point for ADC sampling regardless of the local time. Then the PLL accepts the 1 pulse-per-second (PPS) signal, and generates a desired sampling clock for ADC. It should be noted that due to the relative low frequency of 1 PPS signal, it has a high requirement on the supporting circuits, which are carefully designed to satisfy the standards.

The unique feature of BeagleBone Black with one ARM processor having two additional Programmable Real-time Units (PRU) inside makes it ideal for task of phasor measurements. It is designed that the main ARM CPU would be gathering sampled data in a higher interval (normally 10 ms) and pack it in one XML frame for the following signal processing block in Figure 4. The PRU acts as a middleware between ARM and ADC, by buffering the digital data from a high sampling rate of 12.8 kHz to a lower rate of 0.1 Hz.

5. Conclusion

This paper has presented a test-bed that enables the prototyping and validation of a several core features necessary for future smart grid systems. A full suite of technologies have been implemented, as necessary for provision of complete end-to-end smart grid real-time control strategies. The presented test-bed incorporates a number of novel features based around the modular design for phasor measurement, including state-of-the-art security mechanisms for secure communications across a wide area network. A key benefit of the presented system is the ability to experiment with the full stack of functionality, spanning from the physical –electrical– layer, through standards compliant communications layers, right up to the application layer, where smart grid control functions can be implemented and tested.

6. ACKNOWLEDGMENTS

This work is funded by the EPSRC CAPRICA project (EP/M002837/1).

7. REFERENCES

[1] Eirgrid, “Wind Generation & System Demand Data”, Eirgrid Plc, Dublin, Ireland, Online: www.eirgrid.com, February 2016

[2] Best, R.J., Morrow, D.J., Laverty, D.M., Crossley, P.A.. Synchrophasor Broadcast over Internet Protocol for Distributed Generator Synchronization. IEEE Trans. Power Delivery. Vol. 25, No. 4, October 2010, pp. 2835-2841.

[3] Laverty, D.M.; Best, R.J.; Morrow, D.J., "Loss-of-mains protection system by application of phasor measurement unit technology with experimentally assessed threshold settings," in *Generation, Transmission & Distribution, IET* , vol.9, no.2, pp.146-153, 1 29 2015

[4] Best, R.J.; Morrow, D.J.; Crossley, P.A., "Effect of loading, voltage difference and phase angle on the synchronisation of a small alternator," Electric Power Applications, IET , vol.3, no.6, pp.531,542, November 2009

[5] Best, R.J.; Morrow, D.John; Laverty, D.M.; Crossley, P.A., "Techniques for Multiple-Set Synchronous Islanding Control," in *Smart Grid, IEEE Transactions on* , vol.2, no.1, pp.60-67, March 2011

[6] IEEE Standard for Synchrophasor Data Transfer for Power Systems," in IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005) , vol., no., pp.1-53, Dec. 28 2011

[7] D. M. Laverty, R. J. Best, P. Brogan, I. Al Khatib, L. Vanfretti, and D. J. Morrow, “The OpenPMU Platform for Open-Source Phasor Measurements,” *IEEE Trans. Instrum. Meas.*, vol. 62, no. 4, pp. 701–709, Apr. 2013

[8] “Teensy 3.2 Information.” [Online]. Available: https://www.pjrc.com/teensy/. [Accessed: 1-Nov-2015]

[9] “Raspberry Pi Information.” [Online]. Available: http://www.raspberrypi.org/. [Accessed: 17-Apr-2014]

[10] IEC Standard 61850-90-5: Use of IEC 61850 to transmit synchrophasor information according to IEEE C37.118, IEC/TR 61850-90-5, Edition 1.0, May 2012.

[11] B. Weis, S. Rowles and T. Hardjono, "The Group Domain of Interpretation", in IETF Request for Comments: 6407, October 2011.

[12] E. Rescorla, "Diffie-Hellman Key Agreement Method", in IETF Request for Comments: 2631, June 1999

[13] Wei, D., Lu, Y., Jafari, M., Skare, P. M., & Rohde, K. (2011). Protecting Smart Grid Automation Systems Against Cyberattacks. Smart Grid, IEEE Transactions on, 2(4), 782–795.